Benutzerhandbuch

INSYS icom

Industrielle Datenkommunikation

INSYS

Connectivity Service

Copyright © October 13 INSYS MICROELECTRONICS GmbH

Jede Vervielfältigung dieses Handbuchs ist nicht erlaubt. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

Warenzeichen und Firmenzeichen
Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

MNP ist ein eingetragenes Warenzeichen von Microcom, Inc.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

INSYS®, e-Mobility LSG® und e-Mobility PLC® sind eingetragene Warenzeichen der INSYS MICROELECTRONICS GmbH.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

Herausgeber:
INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Telefon: +49 941 58692 0
Telefax: +49 941 58692 45
E-Mail: info@insys-icom.de
Internet: http://www.insys-icom.de

Datum: Oct-13
Artikelnummer: 31-22-03.182
Version: 1.3
Sprache: DE

1 Allgemeines 5
2 Nutzung des INSYS Connectivity Service 6
3 Erstellen eines VPN-Netzwerks 7
3.1 Anmeldung am INSYS Connectivity Service 8
3.2 Anlegen einer Gruppe 8
3.3 Festlegen der Kommunikationsregeln 9
3.3.1 Kommunikation innerhalb einer Gruppe 9
3.3.2 Kommunikation zwischen den Gruppen 10
3.4 Anlegen eines Geräts 12
3.4.1 Anlegen eines INSYS icom-Geräts 12
3.4.2 Anlegen eines Fremdgeräts 14
4 Konfiguration eines INSYS icom-Routers 16
4.1 Konfiguration mit Hilfe des Schnellstart-Wizards 16
4.2 Konfiguration mit Hilfe der Konfigurationsdatei 20
4.2.1 Herunterladen der Konfigurationsdatei 20
4.2.2 Hochladen der Konfigurationsdatei auf den Router 20
5 Konfiguration von OpenVPN-Clients auf Fremdgeräten 22
6 Aufbauen und Prüfen einer Verbindung 23
6.1 Aufbauen einer Verbindung 23
6.2 Prüfen einer Verbindung 24
7 Weitere Optionen 25
7.1 Geräteverwaltung 25
7.2 Gruppenübersicht 28
7.3 Anzeige der VPN-Daten 29
7.4 Einrichten von Webproxies 30
7.5 Lizenzverwaltung 33
8 Netmapping 35

1 Allgemeines

Dieses Zusatzhandbuch dient als Beschreibung des INSYS Connectivity Service und ist nur zusammen mit dem Benutzerhandbuch und Quick Installation Guide des jeweiligen Routers zu verwenden. Sicherheitshinweise, Technische Daten und Funktionsbeschreibungen sind dem Benutzerhandbuch des jeweiligen Geräts zu entnehmen. Der INSYS Connectivity Service wird von den meisten Routern von INSYS icom unterstützt, unter anderem von:

- MoRoS PRO ab FW 2.8.0
- MLR 2.0 ab FW 2.8.0
- Serien EBW, IMO und RSM

Kontaktieren Sie uns für andere Geräte von INSYS unter support@insys-icom.de.

Für Drittgeräte (PCs/Steuerungen, etc.) empfehlen wir eine OpenVPN-Installation ab Version 2.1.1.

Der INSYS icom Connectivity Service stellt einen sicheren VPN-Dienst zur Verfügung: PCs, Router und lokal angeschlossene Netzwerkgeräte (z.B. Steuerungen, Messgeräte, Webcams) sind in allen Netzen erreichbar und jederzeit ansprechbar.

Sie profitieren vom INSYS Connectivity Service, da Sie keinen eigenen OpenVPN-Server in Ihrem Netz betreiben müssen und somit dessen Betriebs- und Administrationskosten einsparen. Weiterhin ermöglicht er Ihnen eine hochflexible und einfach zu bedienende Rechtevergabe für alle OpenVPN-Clients sowie eine übersichtliche Verwaltung der Geräte im Feld.

Ihre Techniker profitieren von einer automatisierten OpenVPN-Konfiguration der Clients im Feld, die eine Installation ohne weiteres OpenVPN-Know-How ermöglicht. INSYS-Router erhalten mit Hilfe des Schnellstart-Wizard die vollständige OpenVPN-Konfiguration sicher übermittelt.

Ein Vorgehen in folgender Reihenfolge hat sich beim Aufbau eines VPN-Netzwerks mit dem INSYS Connectivity Service als vorteilhaft erwiesen:

1. Planung der Netz-Topologie
2. Anlegen der Geräte im INSYS Connectivity Service
3. Konfiguration der Clients; dabei gibt es für Geräte von INSYS icom zwei Möglichkeiten:
   a) Konfiguration über den Schnellstart-Wizard (vorteilhaft für Geräte, die noch nicht konfiguriert wurden (Werkseinstellungen))
   b) Konfiguration über die Konfigurationsdatei (vorteilhaft für bereits konfigurierte Geräte)

2 Nutzung des INSYS Connectivity Service

Um den INSYS Connectivity Service nutzen zu können, müssen Sie sich zuerst dafür registrieren. Dabei registrieren Sie sich für einen 30-tägigen kostenlosen Testzugang, mit dem Sie maximal 4 Geräte für den Betrieb im OpenVPN-Netzwerk anlegen und verwalten können.
Über den Reiter „Mein VPN“ können Sie die gewünschte Anzahl an Jahreslizenzen bestellen.

Registrierung für den INSYS Connectivity Service

1. ***Öffnen Sie die Seite*** https://connectivity.insys-icom.de

2. ***Wählen Sie Ihre Sprache und klicken Sie auf*** ***Registrieren***.

   ✓ Die Seite für die Registrierung des Zugangs öffnet sich.

3. ***Füllen Sie das Registrierungsformular entsprechend aus und klicken Sie auf*** ***Absenden***.

   ⓘ Der hier eingegebene Firmenname wird danach zum Kundenname, mit dem Sie sich im Schnellstart-Wizard der Geräte von INSYS icom für den INSYS Connectivity Service anmelden.
   Achten Sie auf die korrekte Schreibweise der E-Mail-Adresse und des Passworts sowie die geforderten Pflichtfelder und das Akzeptieren der AGB.

   ✓ An die angegebene E-Mail-Adresse wird eine E-Mail mit einem Aktivierungslink gesendet.

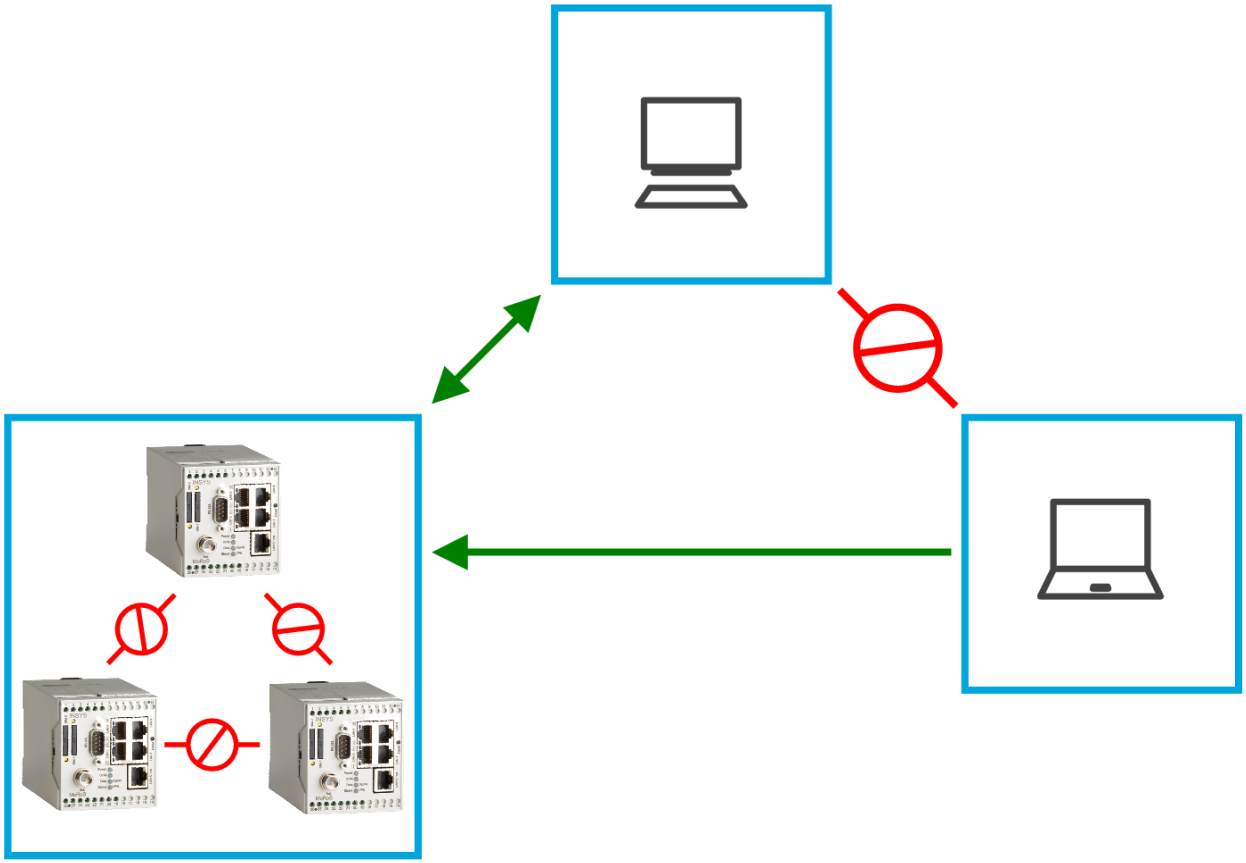
4. ***Klicken Sie auf den Aktivierungslink in der E-Mail um Ihren Zugang freizuschalten.***

   ✓ Sie erhalten eine weitere E-Mail mit Ihren Zugangs- und Kundendaten.

   ✓ Nun können Sie den INSYS Connectivity Service im Testbetrieb nutzen oder Lizenzen für den regulären Betrieb bestellen.

3 Erstellen eines VPN-Netzwerks

Für den Aufbau eines VPN-Netzwerks ist es wichtig, eine geeignete Netz-Topologie im Vorfeld sorgfältig zu planen. Der INSYS Connectivity Service ermöglicht die Einteilung der verschiedenen Geräte in Gruppen. Dabei können Kommunikationsregeln für alle Teilnehmer innerhalb einer Gruppe sowie zwischen den einzelnen Gruppen festgelegt werden. Im Folgenden stellen wir eine beispielhafte Topologie für ein kleineres VPN-Netzwerk vor.



Dabei gibt es die Gruppen Feldgeräte (links), Leitstelle (oben) und Servicetechniker (rechts).

Die Gruppe Feldgeräte enthält drei Router, die zwar ähnliche Funktionen erfüllen, aber untereinander keine Verbindungen aufbauen dürfen, aber Verbindungen zur Leitstelle aufbauen sollen.

Die Gruppe Leitstelle enthält einen Leitstellenrechner des Kunden, der Verbindungen zur Gruppe Feldgeräte aufbauen kann.

In der Gruppe Techniker befindet sich ein Notebook, das Verbindungen zu den Geräten in der Gruppe Feldgeräte aufbauen kann.

Im Folgenden wird erklärt, wie Sie ein VPN-Netzwerk für das hier gezeigte Beispiel mit Hilfe des INSYS Connectivity Service aufbauen.

3.1 Anmeldung am INSYS Connectivity Service

Anmeldung am INSYS Connectivity Service

⇢ Sie haben sich für den INSYS Connectivity Service registriert und die E-Mail mit den Zugangsdaten erhalten

1. ***Gehen Sie auf die Seite*** https://connectivity.insys-icom.de
2. ***Geben Sie Ihre Zugangsdaten ein, wählen Sie Ihre Sprache und klicken Sie auf*** ***Anmelden***.

✓ Damit haben Sie sich erfolgreich am INSYS Connectivity Service angemeldet.

3.2 Anlegen einer Gruppe

Vor dem Anlegen der Geräte ist es sinnvoll, die einzelnen Gruppen anzulegen. Wählen Sie dazu den Reiter „Gruppen“.

ⓘ Nach jedem Anlegen einer Gruppe bzw. nach jeder Änderung an einer Gruppe wird der OpenVPN-Server neu gestartet.

Anlegen einer Gruppe

1. ***Klicken Sie auf*** ***Gruppe hinzufügen***.
2. ***Geben Sie den Namen der Gruppe ein (hier „Feldgeräte“).***
3. ***Klicken Sie auf*** ***OK***.
4. ***Legen Sie auf dieselbe Art die Gruppen „Leitstelle“ und „ServiceTechniker“ an.***
5. ***Löschen Sie die Gruppe „Standardgruppe“, indem Sie auf das Lösch-Symbol (Papierkorb) in der Reihe der Standardgruppe klicken.***

✓ Damit haben Sie die erforderlichen Gruppen angelegt.

3.3 Festlegen der Kommunikationsregeln

Nachdem die Gruppen angelegt wurden, können die Kommunikationsregeln innerhalb der einzelnen Gruppen und zwischen den Gruppen angelegt werden. Diese Regeln können jederzeit geändert werden.

3.3.1 Kommunikation innerhalb einer Gruppe

Da die Mitglieder der Gruppe „Feldgeräte“ untereinander keine Verbindungen aufbauen dürfen, muss dies verboten werden.

Festlegen der internen Kommunikation

1. ***Wählen Sie den Reiter „Gruppen“.***
2. ***Klicken Sie in der Reihe der Gruppe „Feldgeräte“ auf die Schaltfläche in der Spalte „Interne Verbindungen“ um die Regel von „erlaubt“ auf „verboten“ zu ändern.***

ⓘ Die aktuelle Beschriftung der Schaltfläche zeigt an, ob Verbindungen innerhalb dieser Gruppe im Moment „erlaubt“ oder „verboten“ sind.

✓ Damit haben Sie die Kommunikation innerhalb der Gruppen festgelegt.

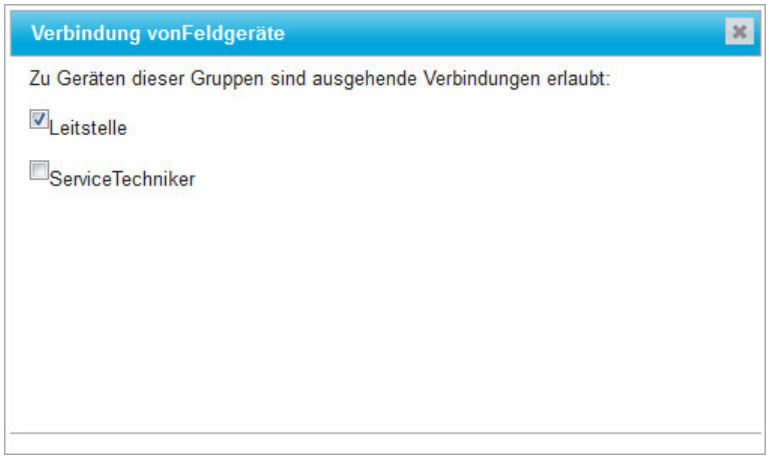
3.3.2 Kommunikation zwischen den Gruppen

Nun ist es erforderlich, die Kommunikationsregeln zwischen den Gruppen festzulegen. Dazu werden die Möglichkeiten für einen Verbindungsaufbau der einzelnen Gruppen explizit erlaubt.

Festlegen der externen Kommunikation

1. ***Um festzulegen, dass Verbindungen von Mitgliedern der Gruppe „Feldgeräte“ zu den Mitgliedern der Gruppe „Leitstelle“ aufgebaut werden dürfen, wählen Sie in der Reihe der Gruppe „Feldgeräte“ die Schaltfläche in der Spalte „Verbindung nach“.***

2. ***Markieren Sie die erlaubte Gruppe „Leitstelle“.***



ⓘ Die Regel wird unmittelbar nach Setzen des Hakens umgesetzt.

3. ***Schließen Sie das Fenster mit „x“.***

✓ Im Gegenzug wurde auch in der Reihe der Gruppe „Leitstelle“ eingetragen, dass Verbindungen von der Gruppe „Feldgeräte“ erlaubt sind.

4. ***Um festzulegen, dass Verbindungen von Mitgliedern der Gruppe „Leitstelle“ zu den Mitgliedern der Gruppe „Feldgeräte“ aufgebaut werden dürfen, wählen Sie in der Reihe der Gruppe „Leitstelle“ die Schaltfläche in der Spalte „Verbindung nach“.***

5. ***Markieren Sie die erlaubte Gruppe „Feldgeräte“ und schließen Sie das Fenster mit „x“.***

6. ***Um festzulegen, dass Verbindungen von Mitgliedern der Gruppe „ServiceTechniker“ zu den Mitgliedern der Gruppe „Feldgeräte“ aufgebaut werden dürfen, wählen Sie in der Reihe der Gruppe „ServiceTechniker“ die Schaltfläche in der Spalte „Verbindung nach“.***

7. ***Markieren Sie die erlaubte Gruppe „Feldgeräte“ und schließen Sie das Fenster mit „x“.***

✓ Damit haben Sie sämtliche Kommunikationsregeln für unser Beispiel innerhalb der einzelnen Gruppen und zwischen den Gruppen festgelegt.

3.4 Anlegen eines Geräts

Nach dem Anlegen der Gruppen und der Festlegung der Kommunikationsregeln können nun die einzelnen Geräte angelegt werden. Dabei wird unterschieden zwischen Geräten von INSYS icom und anderen, fremden Geräten. Dabei kann es sich um PCs, Steuerungen, Kameras, andere Router, etc. handeln, die OpenVPN unterstützen.

ⓘ Nach jedem Anlegen eines Geräts bzw. nach jeder Änderung an einem Gerät wird der OpenVPN-Server neu gestartet.

3.4.1 Anlegen eines INSYS icom-Geräts

Die Feldgeräte von INSYS icom werden in der Gruppe „Feldgeräte“ angelegt.

Anlegen eines INSYS icom-Geräts

⇢ Die entsprechenden Gruppen sind angelegt.

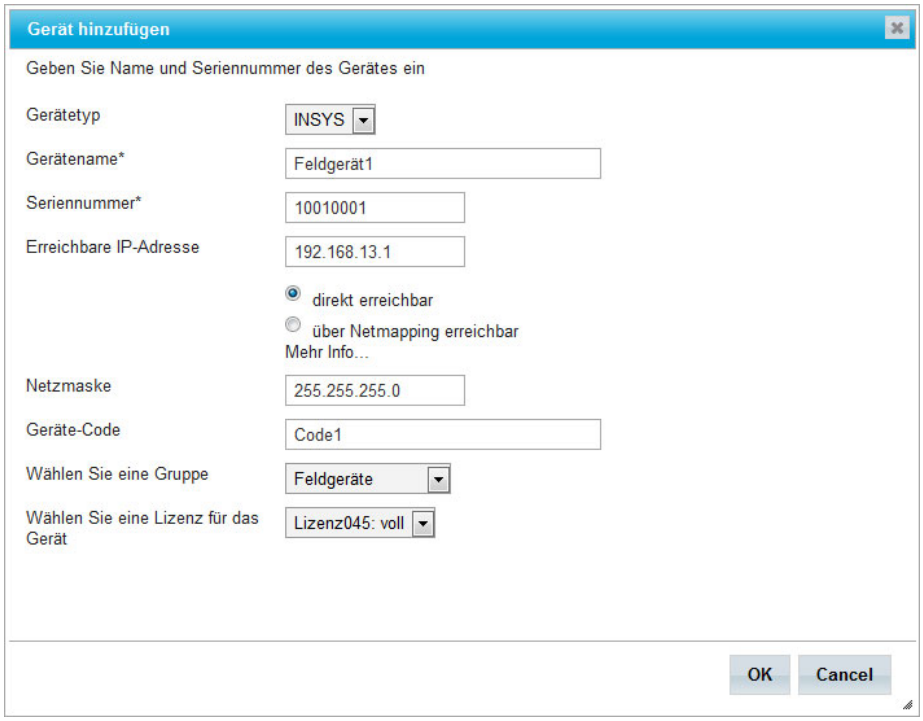
1. ***Wählen Sie den Reiter „Geräte“.***
2. ***Klicken Sie auf*** ***Gerät hinzufügen***.
3. ***Wählen Sie unter „Gerätetyp“ den Typ „INSYS“ aus.***
4. ***Geben Sie unter „Gerätename“ einen Namen ein, der das Gerät so beschreibt, dass es von anderen Geräten unterschieden werden kann.***
5. ***Geben Sie unter „Seriennummer“ die Seriennummer des Geräts ein. Diese finden Sie auf dem Aufkleber am Gerät.***
6. ***Geben Sie unter „Erreichbare Geräte-IP“ optional die lokale IP-Adresse ein, unter der der Router (und weitere lokale Geräte) erreichbar sind.***

   ⓘ Weitere Informationen dazu erhalten Sie unter „Mehr Info…“.
7. ***Geben Sie darunter an, ob das Gerät auf diese IP-Adresse durch den INSYS Connectivity Service umkonfiguriert werden soll (direkt erreichbar), oder ob eine (eindeutige) virtuelle IP-Adresse auf die unveränderte lokale Adresse des Geräts umgeleitet werden soll (über Netmapping erreichbar).***
8. ***Geben Sie unter „Netzmaske“ die Netzmaske für die lokale IP-Adresse des Geräts ein, wenn Sie oben eine IP-Adresse angegeben haben.***
9. ***Geben Sie unter „Geräte-Code“ optional einen Geräte-Code für dieses eine Gerät ein. Dieser wird für die Konfiguration des Geräts über den Schnellstart-Wizard verwendet.***

➢ *Wird hier kein eigener Geräte-Code angegeben, wird der Standard-Code verwendet (konfigurierbar unter dem Reiter „Mein VPN").*

10. Wählen Sie unter „Wählen Sie eine Gruppe" in unserem Beispiel die Gruppe „Feldgeräte" aus.

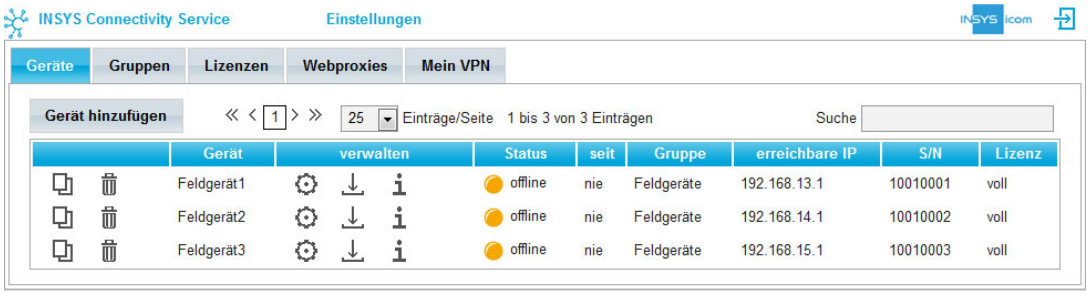
11. Wählen Sie unter „Wählen Sie eine Lizenz für das Gerät" eine der verfügbaren Lizenzen aus.



12. Klicken Sie auf OK.

✓ Damit haben Sie das erste Feldgerät in der Gruppe „Feldgeräte" angelegt.

13. Legen Sie analog dazu die weiteren Feldgeräte an.



✓ Damit haben Sie alle Feldgeräte in der Gruppe „Feldgeräte" angelegt.

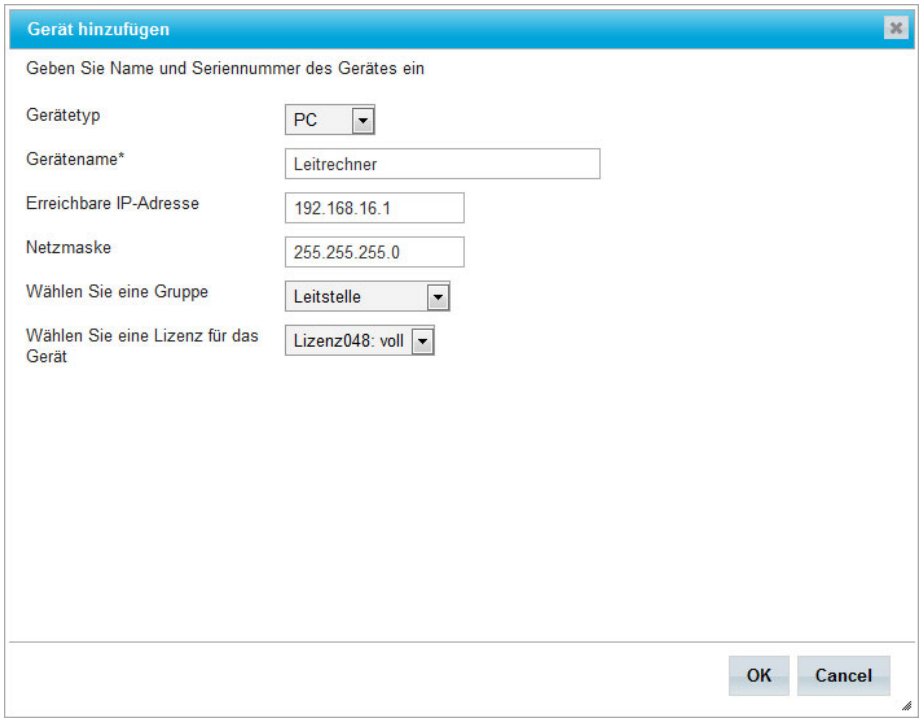
3.4.2 Anlegen eines Fremdgeräts

Der Leitrechner wird als Fremdgerät in der Gruppe „Leitstelle“ angelegt.

Anlegen eines Fremdgeräts

⇢ Die entsprechenden Gruppen sind angelegt.

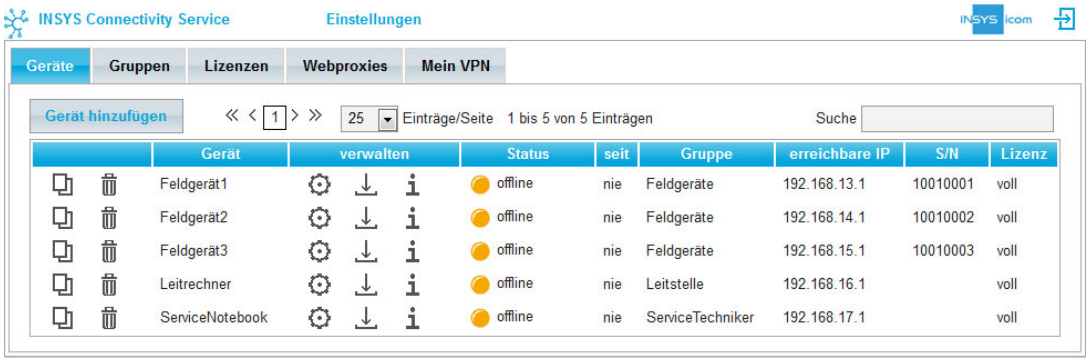
1. ***Wählen Sie den Reiter „Geräte“.***
2. ***Klicken Sie auf Gerät hinzufügen.***
3. ***Wählen Sie unter „Gerätetyp“ den Typ „PC“ aus.***
4. ***Geben Sie unter „Gerätename“ einen Namen ein, der das Gerät so beschreibt, dass es von anderen Geräten unterschieden werden kann.***
5. ***Geben Sie unter „Erreichbare Geräte-IP“ optional die lokale IP-Adresse ein, unter der das Gerät (und weitere lokale Geräte) erreichbar sind.***
6. ***Geben Sie unter „Netzmaske“ die Netzmaske für die lokale IP-Adresse des Geräts ein, wenn Sie oben eine IP-Adresse angegeben haben.***
7. ***Wählen Sie unter „Wählen Sie eine Gruppe“ die Gruppe „Leitstelle“ aus.***
8. ***Wählen Sie unter „Wählen Sie eine Lizenz für das Gerät“ eine der verfügbaren Lizenzen aus.***



9. ***Klicken Sie auf OK.***

✓ Damit haben Sie die Leitstelle in der Gruppe „Leitstelle“ angelegt.

10. Legen Sie analog dazu das Notebook in der Gruppe „ServiceTechniker“ an.



✓ Damit haben Sie alle Geräte für das VPN-Netzwerk angelegt.

4 Konfiguration eines INSYS icom-Routers

Wenn Sie einen INSYS icom-Router im INSYS Connectivity Service angelegt haben, können Sie die Konfiguration für das VPN-Netzwerk einfach auf den Router übertragen. Dies kann mit Hilfe des Schnellstart-Wizards oder manuell durch Hochladen der Konfigurationsdatei auf den Router erfolgen.

4.1 Konfiguration mit Hilfe des Schnellstart-Wizards

Im Folgenden ist die Inbetriebnahme eines Mobilfunkrouters beschrieben. Die Inbetriebnahme anderer Router von INSYS icom erfolgt analog. Der Router muss dazu über eine Firmware ab 2.8.0 verfügen.

Konfiguration mit Hilfe des Schnellstart-Wizards

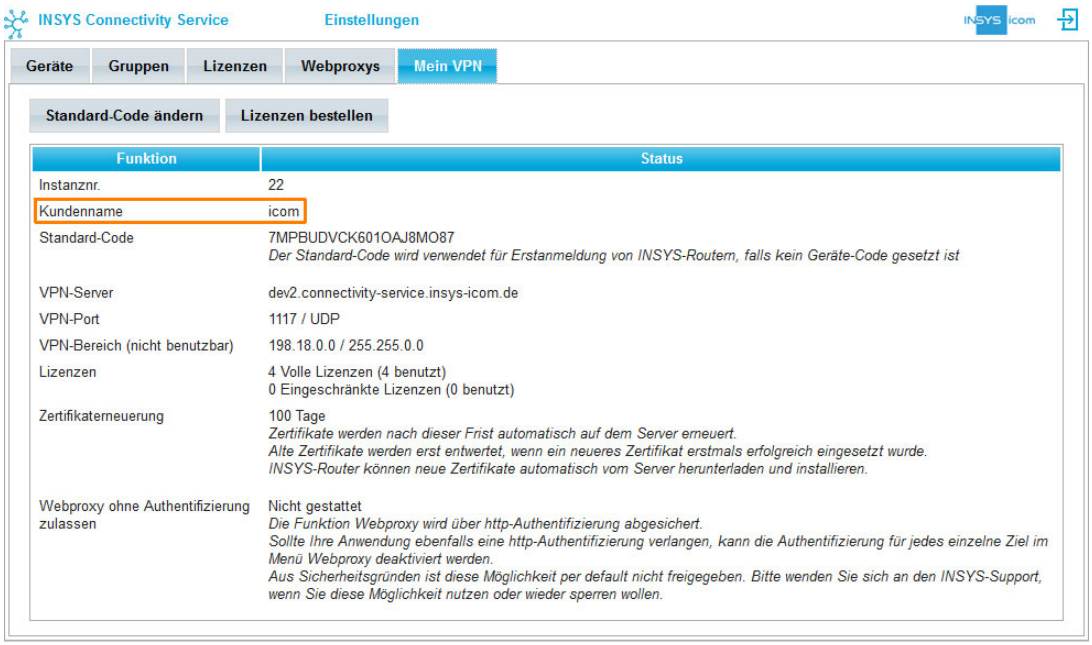
1. ***Nehmen Sie den INSYS icom-Router in Betrieb, wie im zugehörigen Handbuch beschrieben.***

   ⓘ Nach dem ersten Start erscheint auf dem Web-Interface des Routers der Schnellstart-Wizard. Wenn dieser nicht erscheint, ist es erforderlich, den Router auf Werkseinstellungen zurückzusetzen (Menü „System“ und Seite „Reset“ oder Reset-Taster; siehe Handbuch).

2. ***Tragen Sie die Werte im oberen Abschnitt des Schnellstart-Wizards ein, wie im zugehörigen Quick Installation Guide beschrieben.***

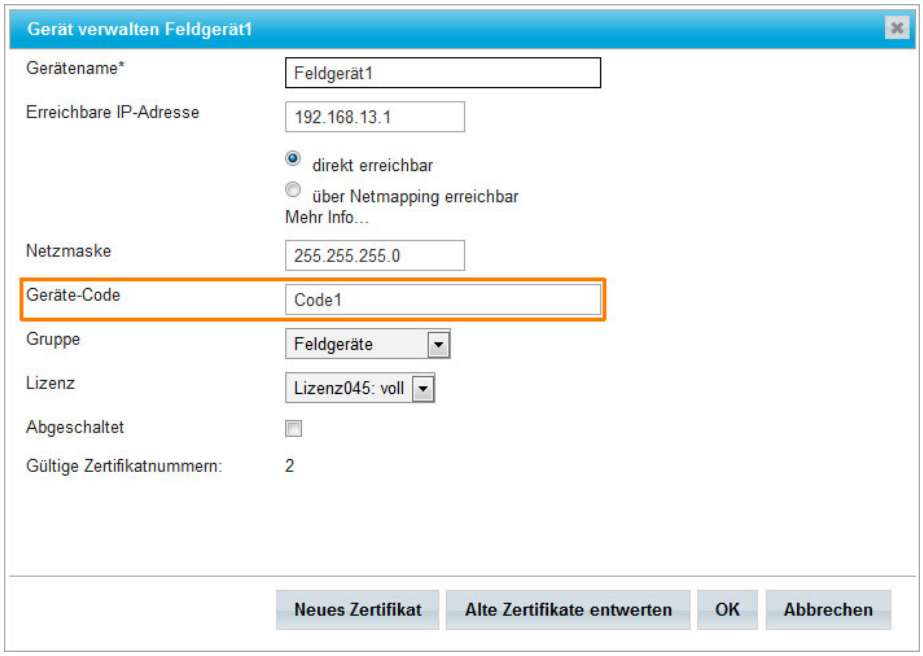
3. ***Geben Sie im Abschnitt „INSYS Connectivity Service“ den Kundennamen ein.***

   ⓘ Der Kundenname wird automatisch aus Ihrem Firmennamen generiert; er enthält keine Leer- und Sonderzeichen. Sie finden ihn über den Reiter „Mein VPN“ unter „Kundename“.

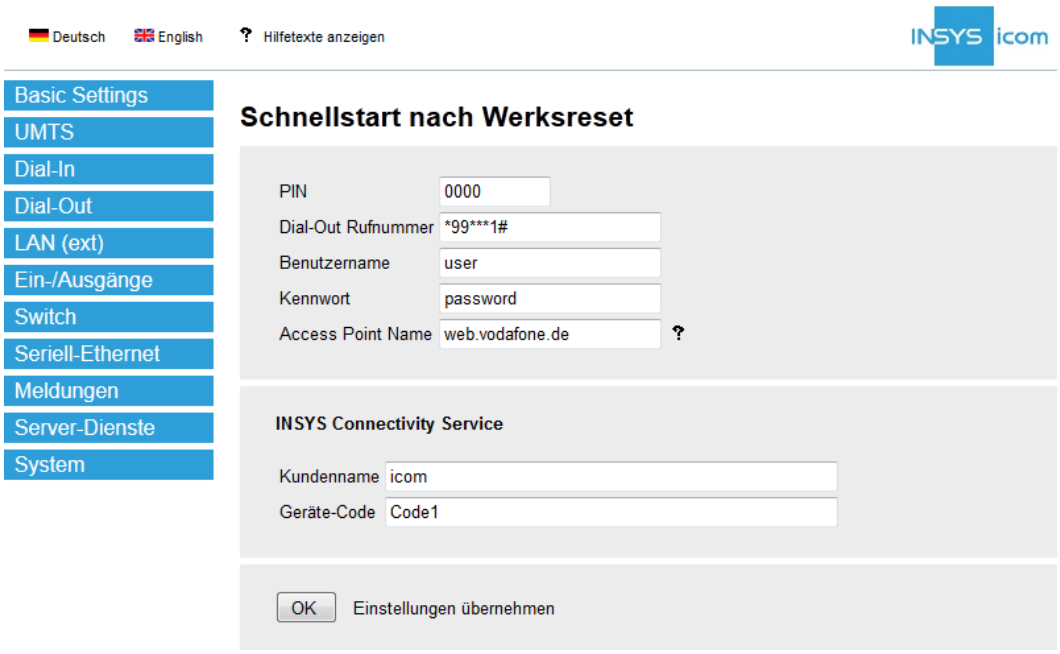

INSYS Connectivity Service
Einstellungen
Geräte
Gruppen
Lizenzen
Webproxys
Mein VPN
Standard-Code ändern
Lizenzen bestellen
Funktion
Status
Instanznr.
22
Kundenname
icom
Standard-Code
7MPBUDVCK601OAJ8MO87
Der Standard-Code wird verwendet für Erstanmeldung von INSYS-Routern, falls kein Geräte-Code gesetzt ist
VPN-Server
dev2.connectivity-service.insys-icom.de
VPN-Port
1117 / UDP
VPN-Bereich (nicht benutzbar)
198.18.0.0 / 255.255.0.0
Lizenzen
4 Volle Lizenzen (4 benutzt)
0 Eingeschränkte Lizenzen (0 benutzt)
Zertifikaterneuerung
100 Tage
Zertifikate werden nach dieser Frist automatisch auf dem Server erneuert.
Alte Zertifikate werden erst entwertet, wenn ein neueres Zertifikat erstmals erfolgreich eingesetzt wurde.
INSYS-Router können neue Zertifikate automatisch vom Server herunterladen und installieren.
Webproxy ohne Authentifizierung zulassen
Nicht gestattet
Die Funktion Webproxy wird über http-Authentifizierung abgesichert.
Sollte Ihre Anwendung ebenfalls eine http-Authentifizierung verlangen, kann die Authentifizierung für jedes einzelne Ziel im Menü Webproxy deaktiviert werden.
Aus Sicherheitsgründen ist diese Möglichkeit per default nicht freigegeben. Bitte wenden Sie sich an den INSYS-Support, wenn Sie diese Möglichkeit nutzen oder wieder sperren wollen.

4. *Geben Sie den Geräte-Code ein.*

ⓘ Dies ist der beim Anlegen des zu konfigurierenden INSYS icom-Geräts im INSYS Connectivity Service gewählte „Geräte-Code“. Diesen finden Sie beispielsweise auch, wenn Sie über den Reiter „Geräte“ in der Reihe des Geräts auf das Verwalten-Symbol (Zahnrad) klicken, um das Fenster des Geräts zu öffnen, unter „Geräte-Code“. Ist kein eigener Geräte-Code für das Gerät vergeben, gilt hier der Standard-Code. Diesen finden Sie über den Reiter „Mein VPN“ unter „Standard-Code“.



5. *Klicken Sie auf* ***OK***.



✓ Der Fortschritt der Konfiguration wird angezeigt.

INSYS Connectivity Service
Die WAN-Verbindung wird hergestellt
Sichere Verbindung zum Server wird hergestellt
Konfiguration wird abgeholt und geprüft
Konfiguration angepasst. Reset wird durchgeführt

✓ Das INSYS icom-Gerät wird durch den INSYS Connectivity Service für das VPN-Netzwerk konfiguriert. Nach erfolgter Konfiguration wird ein Neustart durchgeführt.

ⓘ Beachten Sie, dass der Router nach dem Neustart bereits über die neue IP-Adresse zu erreichen ist, falls eine solche beim Anlegen des Geräts im INSYS Connectivity Service unter „erreichbare Geräte-IP“ eingetragen wurde.

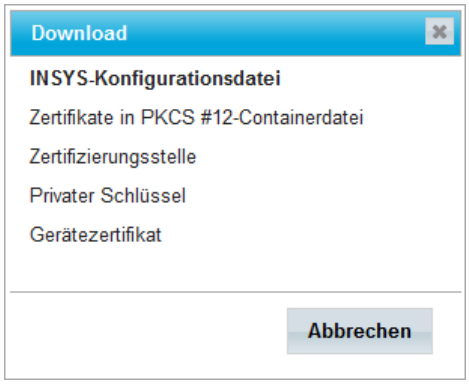
4.2 Konfiguration mit Hilfe der Konfigurationsdatei

Der Router muss dazu über eine Firmware ab 2.4.0 verfügen.

4.2.1 Herunterladen der Konfigurationsdatei

Herunterladen der Konfigurationsdatei

1. ***Wählen Sie im INSYS Connectivity Service den Reiter „Geräte“.***
2. ***Wählen Sie in der Reihe des Gerätes, das Sie konfigurieren möchten, in der Spalte „verwalten“ das Herunterladen-Symbol (Pfeil nach unten).***
3. ***Wählen Sie den Link „INSYS-Konfigurationsdatei“.***



4. ***Speichern Sie die Konfigurationsdatei in ein Verzeichnis Ihrer Wahl ab.***

4.2.2 Hochladen der Konfigurationsdatei auf den Router

Hochladen der Konfigurationsdatei

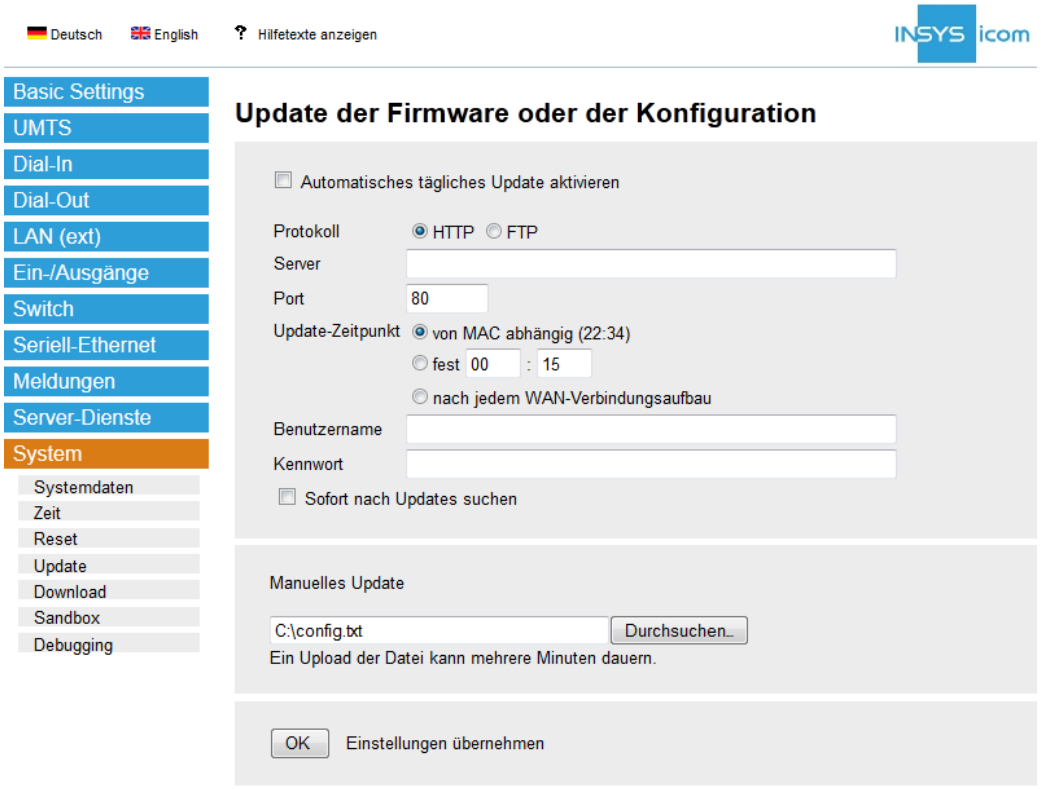
⇢ Sie haben den INSYS icom-Router in Betrieb genommen, wie im zugehörigen Handbuch beschrieben.

1. ***Wechseln Sie im Web-Interface des INSYS icom-Routers im Abschnitt „System“ auf die Seite „Update“.***

   ⓘ Falls Sie eine bereits bestehende VPN-Konfiguration des Routers überschreiben, ist zu beachten, dass im Web-Interface auf der Seite „OpenVPN-Client“ das Feld „Fragmentierung der Tunnelpakete“ zuvor leer sein muss. Ein möglicher Eintrag wird durch die Konfiguration nicht entfernt.

2. ***Klicken Sie im Abschnitt „Manuelles Update“ auf die Schaltfläche Durchsuchen... und öffnen Sie die zuvor abgespeicherte Konfigurationsdatei.***

3. ***Klicken Sie auf OK, um die Konfigurationsdatei auf den Router zu laden.***



4. ***Klicken Sie in der folgenden Sicherheitsabfrage auf Ja, um die Konfiguration des Routers zu überschreiben.***

✓ Das INSYS icom-Gerät wird durch die Konfigurationsdatei für das VPN-Netzwerk konfiguriert. Nach erfolgter Konfiguration wird ein Neustart durchgeführt.

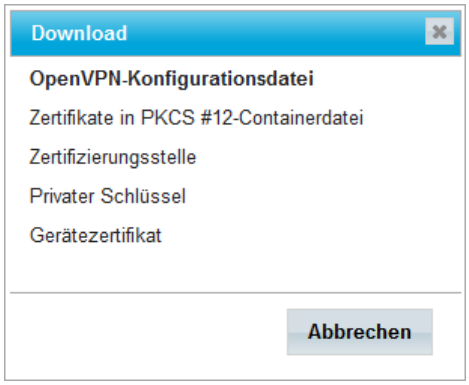
ⓘ Beachten Sie, dass der Router nach dem Neustart bereits über die neue IP-Adresse zu erreichen ist, falls eine solche beim Anlegen des Geräts im INSYS Connectivity Service unter „erreichbare Geräte-IP“ eingetragen wurde.

5 Konfiguration von OpenVPN-Clients auf Fremdgeräten

Wenn Sie ein Fremdgerät (PC, Steuerung, etc.) im INSYS Connectivity Service angelegt haben, können Sie die Konfiguration für das VPN-Netzwerk aus dem INSYS Connectivity Service herunterladen. Auf dem Fremdgerät sollte mindestens die OpenVPN-Version 2.1.1 installiert sein (http://www.insys-icom.de/treiber). Ältere Versionen unterstützen nur ca. 25 Routen.

Konfiguration von OpenVPN-Clients auf Fremdgeräten

1. ***Wählen Sie im INSYS Connectivity Service den Reiter „Geräte“.***
2. ***Wählen Sie in der Reihe des Gerätes, das Sie konfigurieren möchten, in der Spalte „verwalten“ das Herunterladen-Symbol (Pfeil nach unten).***
3. ***Wählen Sie den Link „OpenVPN-Konfigurationsdatei“.***



4. ***Speichern Sie die OpenVPN-Konfigurationsdatei in das Verzeichnis „Config“ der OpenVPN-Installation***

   ⓘ (z.B. Windows XP: C:\Programme\OpenVPN\config; Windows 7: C:\Program Files (x86)\OpenVPN\config)

   ✓ Damit können Sie die OpenVPN GUI (unter Windows 7 / Vista als Administrator) starten und sich mit dem VPN verbinden.

   ⓘ Hinweise zur Installation eines OpenVPN-Clients auf einem Windows PC finden Sie unter http://www.insys-icom.de/OpenVPN-Sicherheit

6 Aufbauen und Prüfen einer Verbindung

Nachdem Sie nun die verschiedenen Teilnehmer für den INSYS Connectivity Service angelegt und konfiguriert haben, können Sie nun die entsprechenden Verbindungen aufbauen und prüfen.

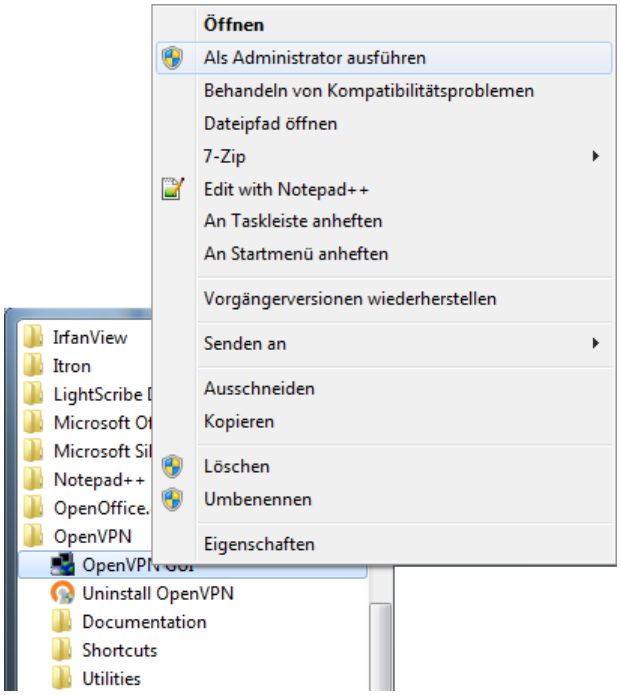
6.1 Aufbauen einer Verbindung

Im Folgenden ist der Aufbau einer Verbindung vom Leitrechner (Fremdgerät) zum INSYS Connectivity Service beschrieben. INSYS icom-Geräte verbinden sich automatisch mit dem INSYS Connectivity Service.

Aufbau einer Verbindung zum INSYS Connectivity Service

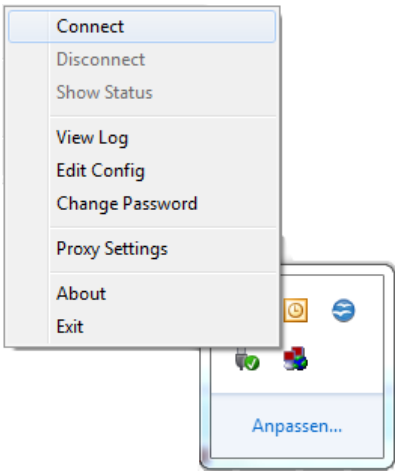
1. ***Öffnen Sie die OpenVPN GUI auf dem „Leitrechner".***

   ⓘ Unter Windows 7 / Vista muss unbedingt wie im Screenshot gezeigt die OpenVPN GUI „als Administrator" ausgeführt werden (rechte Maustaste – Kontextmenü).



2. ***Klicken Sie mit der rechten Maustaste auf das Symbol der OpenVPN GUI und wählen Sie „Connect“.***

   ⓘ Wenn Sie mehrere OpenVPN-Konfigurationen angelegt haben, müssen Sie hier „Leitrechner -> Connect“ wählen.



   ✓ Der Leitrechner verbindet sich mit dem INSYS Connectivity Service.

6.2 Prüfen einer Verbindung

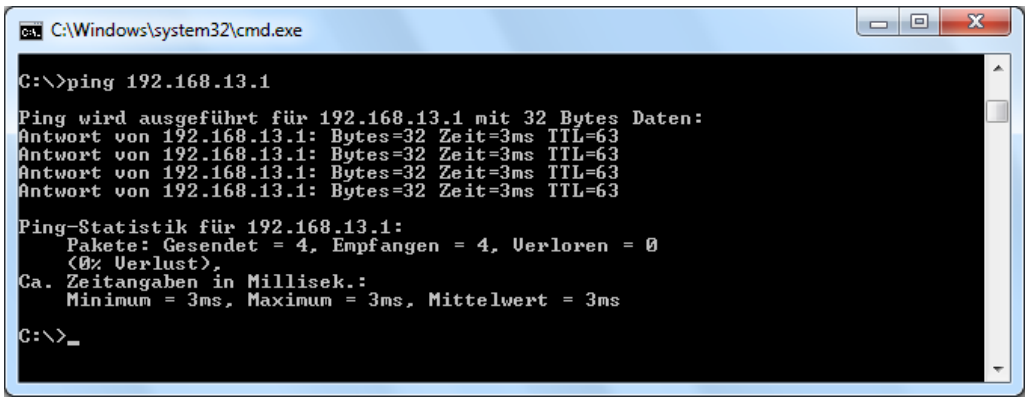
Im Folgenden ist beschrieben, wie Sie die Verbindung vom Leitrechner zu einem Feldgerät prüfen können.

Prüfen einer Verbindung über den INSYS Connectivity Service

1. ***Öffnen Sie die Eingabeaufforderung auf dem „Leitrechner“.***

2. ***„Pingen“ Sie die IP-Adresse eines Feldgeräts.***

   ⓘ Die IP-Adresse ist hier die Adresse, die Sie beim Anlegen des Feldgeräts im INSYS Connectivity Service angegeben haben.


C:\Windows\system32\cmd.exe
C:\>ping 192.168.13.1
Ping wird ausgeführt für 192.168.13.1 mit 32 Bytes Daten:
Antwort von 192.168.13.1: Bytes=32 Zeit=3ms TTL=63
Antwort von 192.168.13.1: Bytes=32 Zeit=3ms TTL=63
Antwort von 192.168.13.1: Bytes=32 Zeit=3ms TTL=63
Antwort von 192.168.13.1: Bytes=32 Zeit=3ms TTL=63
Ping-Statistik für 192.168.13.1:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 3ms, Maximum = 3ms, Mittelwert = 3ms
C:\>

   ✓ Ein erfolgreicher Ping bestätigt Ihnen die Verbindung.

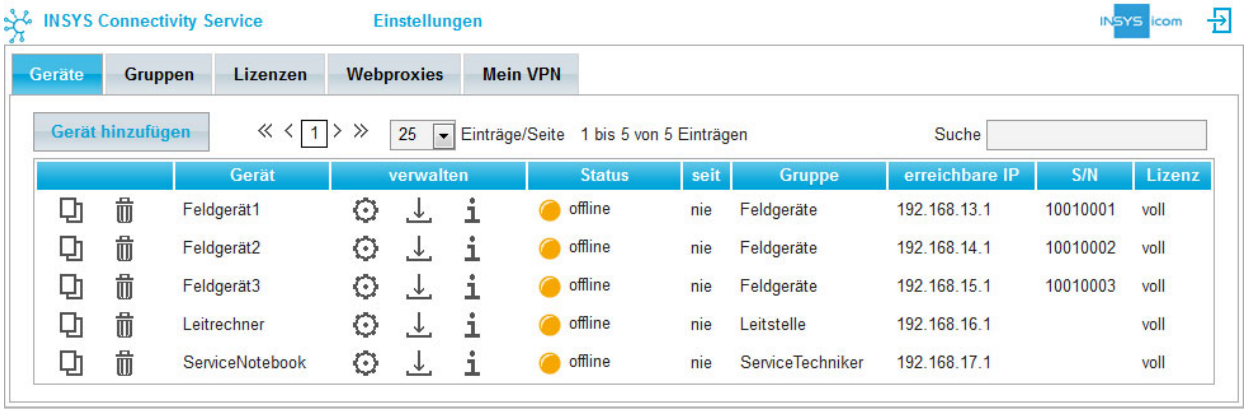
   ➢ *Alternativ können Sie auch die IP-Adresse in den Browser eingeben, um zu sehen, ob Sie auf das Web-Interface des Feldgeräts zugreifen können.*

7 Weitere Optionen

Abgesehen von den im vorangegangenen Beispiel verwendeten Funktionen stehen Ihnen im INSYS Connectivity Service noch weitere Optionen zur Verfügung.

7.1 Geräteverwaltung

Eine Übersicht über alle angelegten Geräte erhalten Sie, wenn Sie den Reiter „Geräte“ wählen.

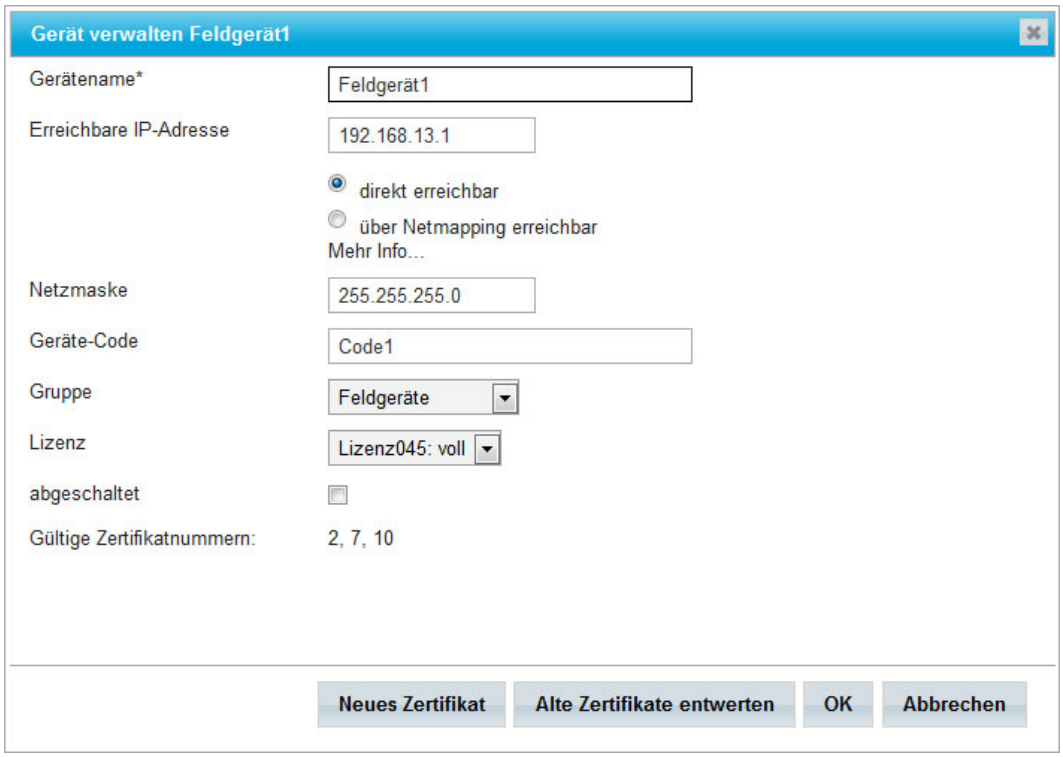


Auf dieser Seite können Sie über die Schaltfläche „Gerät hinzufügen“ weitere Geräte hinzufügen.

Über das Kopieren-Symbol (zwei Blätter) in der Reihe eines Geräts können Sie ein weiteres Gerät auf Basis der Daten dieses Geräts hinzufügen.

Über das Löschen-Symbol (Papierkorb) in der Reihe eines Geräts können Sie dieses Gerät entfernen.

Über das Verwalten-Symbol (Zahnrad) in der Reihe eines Geräts können Sie die Eigenschaften dieses Geräts bearbeiten. Hier können Sie auch ein neues Zertifikat für dieses Gerät erstellen lassen sowie das alte Zertifikat zurückziehen.



Über das Herunterladen-Symbol (Pfeil nach unten) in der Reihe eines Geräts können Sie eine Konfigurationsdatei für dieses Gerät sowie die Zertifikate und Schlüssel sowohl in einer Containerdatei als auch einzeln herunterladen.

Über das Info-Symbol (i) in der Reihe eines Geräts werden der Datendurchsatz sowie die feste VPN-IP-Adresse dieses Geräts angezeigt.

In der Spalte „Status“ wird der aktuelle Zustand des Geräts angegeben. Das Gerät kann online, offline oder ohne Lizenz sein.

In der Spalte „seit“ wird angegeben, seit wann sich das Gerät im aktuellen Zustand befindet.

In der Spalte „Gruppe“ wird angegeben, welcher Gruppe das Gerät zugeordnet ist.

In der Spalte „erreichbare IP“ wird die IP-Adresse angegeben, unter welcher das Gerät erreichbar ist.

In der Spalte „S/N“ wird die Seriennummer des Geräts angezeigt (nur für INSYS-Geräte).

In der Spalte „Lizenz“ wird der Lizenzumfang angegeben.

7.2 Gruppenübersicht

Eine Übersicht über alle angelegten Gruppen erhalten Sie, wenn Sie den Reiter „Gruppen“ wählen.

Auf dieser Seite können Sie über die Schaltfläche „Gruppe hinzufügen“ weitere Gruppen hinzufügen.

Über das Kopieren-Symbol (zwei Blätter) in der Reihe einer Gruppe können Sie eine weitere Gruppe auf Basis der Daten dieser Gruppe hinzufügen.

Über das Löschen-Symbol (Papierkorb) in der Reihe einer Gruppe können Sie diese Gruppe entfernen.

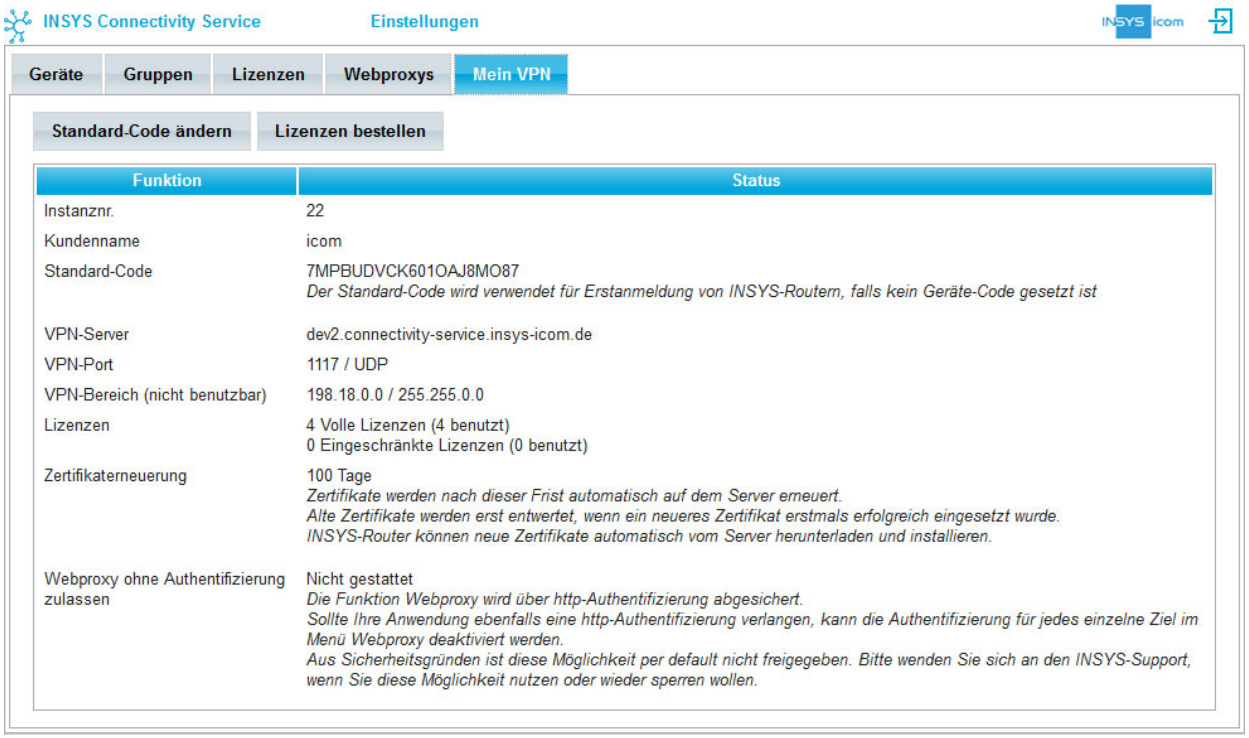
Über die Schaltfläche in der Spalte „Interne Verbindungen“ einer Gruppe können Sie festlegen, ob Verbindungen zwischen den Mitgliedern dieser Gruppe erlaubt oder verboten sind.

Über die Schaltfläche in der Spalte „Verbindung von“ einer Gruppe können Sie diejenigen Gruppen festlegen, von denen aus Verbindungen zu dieser Gruppe erlaubt sind.

Über die Schaltfläche in der Spalte „Verbindung nach“ einer Gruppe können Sie diejenigen Gruppen festlegen, zu denen Verbindungen von dieser Gruppe aus erlaubt sind.

7.3 Anzeige der VPN-Daten

Daten des VPN-Netzwerks, die beispielsweise für die manuelle Konfiguration von Fremdgeräten wichtig sein können, werden angezeigt, wenn Sie den Reiter „Mein VPN“ wählen.


INSYS Connectivity Service
Einstellungen
Geräte
Gruppen
Lizenzen
Webproxys
Mein VPN
Standard-Code ändern
Lizenzen bestellen
Funktion
Status
Instanznr.
22
Kundenname
icom
Standard-Code
7MPBUDVCK601OAJ8MO87
Der Standard-Code wird verwendet für Erstanmeldung von INSYS-Routern, falls kein Geräte-Code gesetzt ist
VPN-Server
dev2.connectivity-service.insys-icom.de
VPN-Port
1117 / UDP
VPN-Bereich (nicht benutzbar)
198.18.0.0 / 255.255.0.0
Lizenzen
4 Volle Lizenzen (4 benutzt)
0 Eingeschränkte Lizenzen (0 benutzt)
Zertifikaterneuerung
100 Tage
Zertifikate werden nach dieser Frist automatisch auf dem Server erneuert.
Alte Zertifikate werden erst entwertet, wenn ein neueres Zertifikat erstmals erfolgreich eingesetzt wurde.
INSYS-Router können neue Zertifikate automatisch vom Server herunterladen und installieren.
Webproxy ohne Authentifizierung zulassen
Nicht gestattet
Die Funktion Webproxy wird über http-Authentifizierung abgesichert.
Sollte Ihre Anwendung ebenfalls eine http-Authentifizierung verlangen, kann die Authentifizierung für jedes einzelne Ziel im Menü Webproxy deaktiviert werden.
Aus Sicherheitsgründen ist diese Möglichkeit per default nicht freigegeben. Bitte wenden Sie sich an den INSYS-Support, wenn Sie diese Möglichkeit nutzen oder wieder sperren wollen.

ⓘ Die Parameter „Kundenname“ und „Standard-Code“ sind für den Schnellstart-Wizard der INSYS icom-Geräte erforderlich.
Der VPN-Port gibt an, auf welchem UDP-Port der INSYS Connectivity Service OpenVPN-Tunnel entgegennimmt. Der Benutzer muss gewährleisten, dass UDP-Pakete an diesen Port gesendet werden können (z.B. diesen Port in der Firewall öffnen).

7.4 Einrichten von Webproxies

Der INSYS Connectivity Service ermöglicht das Einrichten von Webproxies. Webproxies vermitteln den Zugriff auf einen Web-Dienst, der im VPN erreichbar ist, über das http-Protokoll. Damit kann von nahezu jedem PC oder Smartphone mit Internet-Zugang aus auf viele http-fähige Geräte (z.B. IP-Kameras) zugegriffen werden. Die Übertragung der Daten erfolgt verschlüsselt über https. Im folgenden Beispiel soll ein Webproxy für eine Kamera eingerichtet werden, die sich im lokalen Netz von Feldgerät1 befindet.

Hinweis

Sicherheitsgefahr!

Bei Verwendung eines Webproxy ist die betreffende Anwendung über das Internet erreichbar.

Die verschlüsselte Verbindung ist nur noch durch ein Passwort gegen Zugriffe aus dem Internet geschützt. Wählen Sie ein möglichst sicheres Passwort und ändern Sie das Passwort regelmäßig. Wir empfehlen diese Funktion nicht für sicherheitskritische Anwendungen.

Einrichten eines Webproxies

⇢ Der INSYS Connectivity Service ist entsprechend konfiguriert.

1. ***Wählen Sie den Reiter „Webproxys“.***
2. ***Klicken Sie auf*** ***Webproxy hinzufügen***.
3. ***Wählen Sie unter „Gerät“ das Gerät aus, in dessen Netz sich das Gerät befindet, für das der Webproxy eingerichtet werden soll.***
4. ***Geben Sie unter „Name“ einen beschreibenden Namen für den Webproxy ein.***
5. ***Geben Sie unter „IP-Adresse im VPN“ die IP-Adresse an, unter der das Gerät im VPN erreicht wird.***
6. ***Geben Sie unter „Port“ optional einen Port an, über den auf das Gerät zugegriffen werden kann.***
7. ***Markieren Sie die Checkbox „Zugriff ohne Passwort“, wenn der Zugriff auf das Gerät ohne Passwort erfolgen soll.***

   ⓘ Kontaktieren Sie unseren Support, um diese Option für Sie zu aktivieren. Eine Deaktivierung des Passwortschutzes ist beispielsweise erforderlich, wenn die Kamera in diesem Beispiel ebenfalls eine http-Authentifizierung verlangt, da eine zweistufige Authentifizierung in einer Browser-Session nicht möglich ist.

Hinweis

Sicherheitsgefahr!

Nach Deaktivierung des Passwortschutzes ist die betreffende Anwendung ohne Schutz durch den INSYS Connectivity Service über das Internet erreichbar.

Eine Sicherheit kann nur noch durch die Applikation selbst hergestellt werden. Die regelmäßige Prüfung der Applikation auf Sicherheitslücken ist daher unbedingt erforderlich. Wir empfehlen diese Funktion nicht für sicherheitskritische Anwendungen.

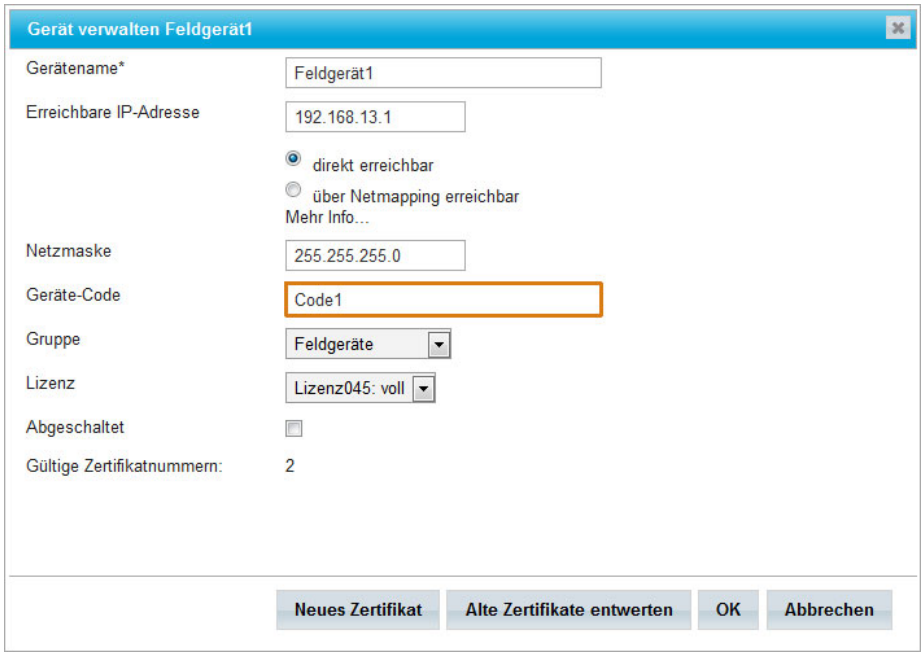
Webproxy hinzufügen
Fügen Sie einen neuen Webproxy hinzu.
Gerät
Feldgerät1
Name
Kamera1
IP-Adresse im VPN
192.168.13.100
Port
80
Zugriff ohne Passwort
Die Funktion Webproxy wird über http-Authentifizierung abgesichert. Sollte Ihre Anwendung ebenfalls eine http-Authentifizierung verlangen, kann die Authentifizierung für jedes einzelne Ziel im Menü Webproxy deaktiviert werden. Aus Sicherheitsgründen ist diese Möglichkeit per default nicht freigegeben. Bitte wenden Sie sich an den INSYS-Support, wenn Sie diese Möglichkeit nutzen oder wieder sperren wollen.
OK

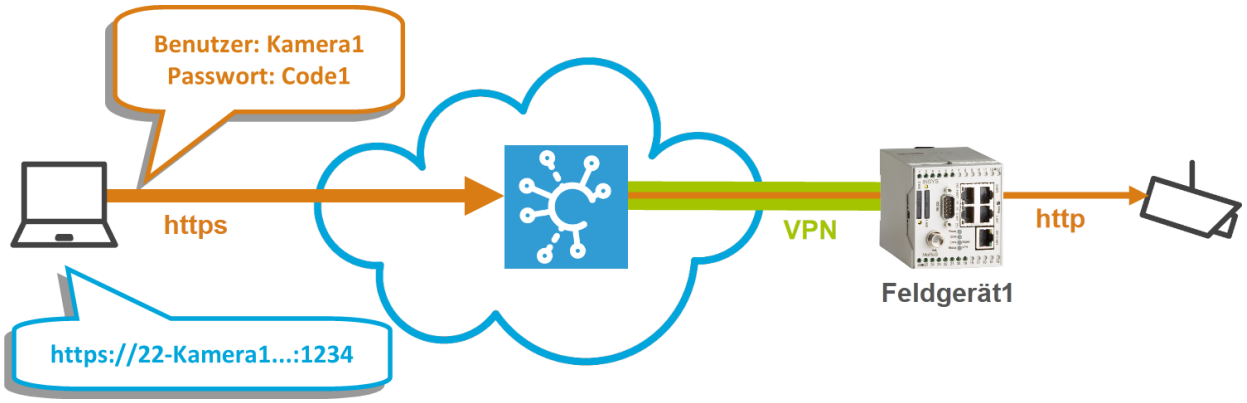
8. ***Klicken Sie auf*** ***OK***.

✓ Damit haben Sie den Webproxy angelegt.

Über die in der Übersicht der Webproxies angezeigte URL kann nun ohne einen VPN-Zugang auf die Kamera hinter Feldgerät1 zugegriffen werden. Der Benutzername für die Authentifizierung ist entweder der Name des Webproxies (in diesem Fall „Kamera1“) oder die Seriennummer des Kommunikationsgeräts, an das das Gerät angeschlossen ist, auf das zugegriffen werden soll (in diesem Fall die Seriennummer von Feldgerät1). Das Passwort ist der Geräte-Code des Kommunikationsgeräts. Wenn kein Geräte-Code konfiguriert ist, gilt der Standard-Code.

INSYS Connectivity Service
Einstellungen
Geräte
Gruppen
Lizenzen
Webproxies
Mein VPN
Webproxy hinzufügen
25
Einträge/Seite
1 bis 1 von 1 Einträgen
Suche
Name
Aufruf Webproxy
IP im VPN
Port
Gerät
Kamera1
offline --
https://22-Kamera1.dev2.connectivity-service.insys-icom.de/
192.168.13.100
80
Feldgerät1


Gerät verwalten Feldgerät1
Gerätename*
Feldgerät1
Erreichbare IP-Adresse
192.168.13.1
direkt erreichbar
über Netmapping erreichbar
Mehr Info...
Netzmaske
255.255.255.0
Geräte-Code
Code1
Gruppe
Feldgeräte
Lizenz
Lizenz045: voll
Abgeschaltet
Gültige Zertifikatnummern:
2
Neues Zertifikat
Alte Zertifikate entwerten
OK
Abbrechen


Benutzer: Kamera1
Passwort: Code1
https
VPN
http
Feldgerät1
https://22-Kamera1...:1234

7.5 Lizenzverwaltung

Der INSYS Connectivity Service verfügt über verschiedene flexible Lizenzierungsmodelle.

Die unbegrenzte Lizenz ist gedacht für eine dauerhafte und regelmäßige Nutzung.

Die beschränkte Lizenz dient zur Sicherstellung der Erreichbarkeit für Geräte, auf die in der Regel nicht zugegriffen wird. Diese Lizenz erlaubt die Verbindung zum INSYS Connectivity Service an 12 Tagen pro Jahr.

Eine Übersicht über Ihre Lizenzen erhalten Sie, wenn Sie den Reiter „Lizenzen“ wählen.

Auf dieser Seite können Sie über die Schaltfläche „Lizenzen bestellen“ direkt zusätzliche Lizenzen bestellen.

Über das Verwalten-Symbol (Zahnrad) in der Reihe der jeweiligen Lizenz können Sie diese Lizenz einem anderen Gerät zuweisen und diese Lizenz freigeben.

Über das Info-Symbol (i) in der Reihe der jeweiligen Lizenz wird ein Protokoll über die Nutzung dieser Lizenz angezeigt.

Wenn Sie auf die Schaltfläche mit dem Namen der Lizenz klicken, können Sie den Lizenznamen verändern.

In der Spalte „Umfang“ wird der Lizenzumfang angegeben. Neben den unbegrenzten Lizenzen stehen auch beschränkte Lizenzen zur Verfügung. Diese sind auf 12 Nutzungstage pro Jahr beschränkt, wobei sich der Nutzungstag auf UTC bezieht, d.h. ein Nutzungstag beginnt um 00:00 UTC, also z.B. 01:00 MEZ oder 02:00 MESZ. Die Anzahl der bereits genutzten Tage wird in der Spalte „Nutzung“ angezeigt. Bei Erreichen von 75% und 100% der Nutzung verschickt das System außerdem eine Warnung per E-Mail.

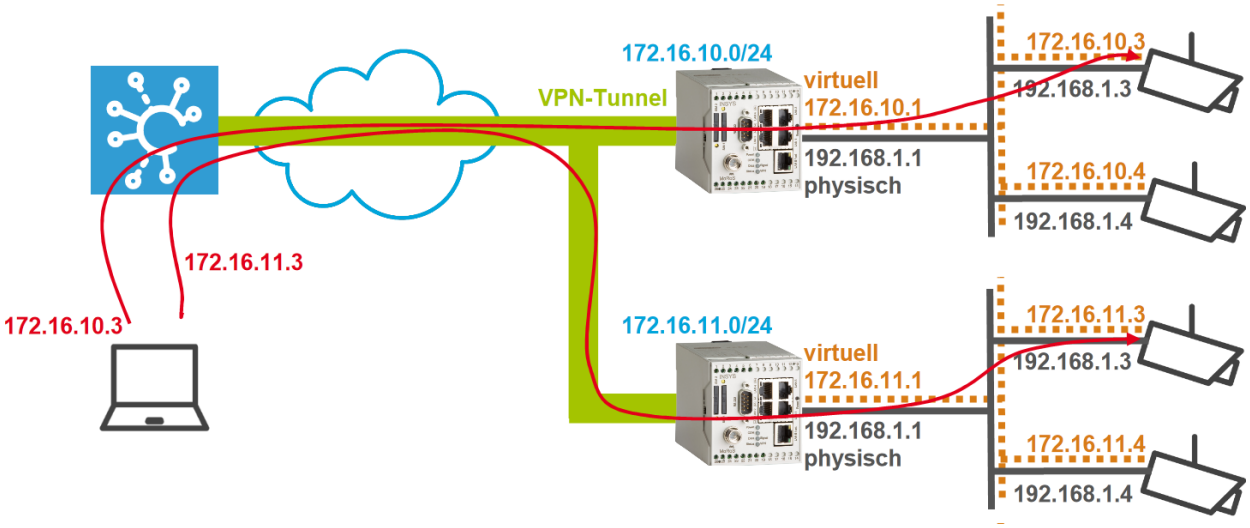
In der Spalte „Gültig bis“ wird der Gültigkeitszeitraum der Lizenz angegeben.

In der Spalte „Gerät“ wird das Gerät angegeben, dem diese Lizenz zugewiesen wurde.

8 Netmapping

Die Verwendung von Netmapping ermöglicht, dass die Geräte im lokalen Netzwerk hinter einem INSYS-Router nicht umkonfiguriert werden müssen. Dabei wird dem lokalen Netzwerk eine virtuelle Netzadresse zugewiesen. Geräte im lokalen Netzwerk können anschließend über den INSYS Connectivity Service mit der virtuellen Adresse angesprochen werden. Der Router tauscht den Netzwerkanteil der virtuellen IP-Adresse gegen den Netzwerkanteil des lokalen Netzwerkes aus und leitet das Paket an das Ziel weiter.

Netmapping wird im Menü „Basic Settings“ auf der Seite „IP-Adresse (LAN)“ des INSYS-Routers konfiguriert. Weitere Hinweise dazu finden Sie im Benutzerhandbuch des Routers.



In obigem Beispiel wurde in den Routern Netmapping aktiviert und die virtuellen Netzadressen „172.16.10.0“ im oberen lokalen Netz und „172.16.11.0“ im unteren lokalen Netz konfiguriert. Dadurch sind die Geräte im lokalen Netzwerk (192.168.1.0/24) auch über die virtuelle Netzadresse (172.16.10.0/24 oben und 172.16.11.0/24 unten) erreichbar und müssen nicht umkonfiguriert werden, obwohl sie dieselben lokalen Netzwerkadressen haben. Die obere Kamera mit der lokalen Netzwerkadresse 192.168.1.3 kann somit von außen über die Adresse 172.16.10.3 und die untere über die Adresse 172.16.11.3 erreicht werden.